Mitigation of Abuse in gTLDs

GAC PSWG | ICANN 57 | 5 November 2016

Goals and Expected Outcomes of this Session

1
Update on
current trends
in abuse of the DNS

2
Discussion of
industry practices
for mitigating
abuse of the DNS

3
Sharing views
for consideration in
ongoing reviews
and initiatives

Session Chaired by:
Alice Munyua - African Union Commission GAC Representative, PSWG co-Chair

Discussion Moderated by:
Robert Flaim, GAC PSWG Member
Executive Office Liaison, Science and Technology Branch Executive Office
Federal Bureau of Investigation, United States

Agenda & Speakers

- Abuse of the DNS
  - Definition — Robert Flaim (GAC PSWG, US FBI)
  - Illustration — Drew Bagley (Secure Domain Foundation)

- Mitigation of Abuse: Current industry practices
  - ICANN — Allen Grogan, Carlos Alvarez (SSR)
  - gTLD Registries — Brian Cimbolic (PIR), Statton Hammock (Rightside)
  - ccTLD Registries — Giovanni Seppia (EURid, .eu)
  - Registrars — Michele Neylon (Blacknight)
  - Business — Denise Michel (Facebook)

- Discussion with Audience

Abuse of the DNS: Definition

- The GAC Safeguards on New gTLDs (Beijing Communiqué, 11 April 2013) defines abuse of the DNS as:

  "*domains […] used to perpetrate security threats, such as:*
  - *pharming,*
  - *phishing,*
  - *malware*
  - *and botnets*"

- This definition is the basis of Specification 11 section 3b of the New gTLD Registry Agreement

Abuse of the DNS: Illustration

Drew Bagley (Secure Domain Foundation)

Abuse Mitigation Current Practices: ICANN

Allen Grogan (Chief Contractual Compliance Officer)

ICANN's Mission and Bylaws & Key contract provisions re abuse

Allen R. Grogan | ICANN 57 | 5 November 2016

Mission – explicit limitations

1.1(b) ICANN shall not act outside its Mission.

1.1 (c) ICANN shall not regulate (i.e., impose rules and restrictions on) services that use the Internet's unique identifiers or the content that such services carry or provide, outside the express scope of Section 1.1(a). For the avoidance of doubt, ICANN does not hold any governmentally authorized regulatory authority.

Mission – “grandfathering”

Notwithstanding any provision of the Bylaws to the contrary, the terms and conditions of certain agreements, and ICANN’s performance of its obligations or duties thereunder, may not be challenged by any party in any proceeding against ICANN on the basis that such terms and conditions conflict with, or are in violation of, ICANN’s Mission or otherwise exceed the scope of ICANN’s authority or powers the Bylaws or ICANN’s Articles of Incorporation

Mission – agreements “grandfathered”

all registry agreements and registrar accreditation agreements between ICANN and registry operators or registrars in force on 1 October 2016, including, in each case, any terms or conditions therein that are not contained in the underlying form of registry agreement and registrar accreditation agreement;

any registry agreement or registrar accreditation agreement to the extent its terms do not vary materially from the form of registry agreement or registrar accreditation agreement that existed on 1 October 2016;

any renewals of agreements described above pursuant to their terms and conditions for renewal

ICANN has the ability to negotiate, enter into and enforce agreements, including public interest commitments, with any party in service of its Mission

Section 3.7.7.9 of the 2013 RAA

The Registration Agreement with the Registered Name Holder must include a provision by which “the Registered Name Holder shall represent that, to the best of the Registered Name Holder's knowledge and belief, neither the registration of the Registered Name nor the manner in which it is directly or indirectly used infringes the legal rights of any third party.”

Section 3.7.7 obligates the Registrar to “use commercially reasonable efforts to enforce compliance with the provisions of the registration agreement between Registrar and any Registered Name Holder that relate to implementing” [this requirement]

Section 3.18.1 of the 2013 RAA

Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity. Registrar shall publish an email address to receive such reports on the home page of Registrar's website (or in another standardized place that may be designated by ICANN from time to time). Registrar shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse.

Section 3.18.2 of the 2013 RAA

Registrar shall establish and maintain a dedicated abuse point of contact, including a dedicated email address and telephone number that is monitored 24 hours a day, seven days a week, to receive reports of Illegal Activity by law enforcement, consumer protection, quasi-governmental or other similar authorities designated from time to time by the national or territorial government of the jurisdiction in which the Registrar is established or maintains a physical office. Well-founded reports of Illegal Activity submitted to these contacts must be reviewed within 24 hours by an individual who is empowered by Registrar to take necessary and appropriate actions in response to the report. In responding to any such reports, Registrar will not be required to take any action in contravention of applicable law.

Section 3.18.3 of the 2013 RAA

Registrar shall publish on its website a description of its procedures for the receipt, handling, and tracking of abuse reports. Registrar shall document its receipt of and response to all such reports. Registrar shall maintain the records related to such reports for the shorter of two (2) years or the longest period permitted by applicable law, and during such period, shall provide such records to ICANN upon reasonable notice.

Section 4, Spec. 6, new gTLD Registry Agreement

4.1 **Abuse Contact**. Registry Operator shall provide to ICANN and publish on its website its accurate contact details including a valid email and mailing address as well as a primary contact for handling inquiries related to malicious conduct in the TLD, and will provide ICANN with prompt notice of any changes to such contact details.

4.2 **Malicious Use of Orphan Glue Records**. Registry Operator shall take action to remove orphan glue records (as defined at http://www.icann.org/en/committees/security/sac048.pdf) when provided with evidence in written form that such records are present in connection with malicious conduct.

Section 3a, Spec 11, new gTLD Registry Agreement

Registry Operator will include a provision in its Registry-Registrar Agreement that requires Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law, and providing (consistent with applicable law and any related procedures) consequences for such activities including suspension of the domain name.

This provision is a Public Interest Commitment ("PIC").

Enforcement of Public Interest Commitments

Public Interest Commitments ("PICs") are part of the contract between ICANN and the Registry Operator and are subject to enforcement by ICANN's contractual compliance department in the ordinary course of its enforcement activities.

The Public Interest Commitments Dispute Resolution Procedure ("PICDRP") http://newgtlds.icann.org/en/applicants/agb/picdrp-19dec13-en.pdf provides a potential alternative or parallel mechanism for a harmed party to pursue remedies, but it does not preclude or limit ICANN from enforcing the PICs through its normal contractual compliance process and timetable.

Enforcement of Public Interest Commitments

Nothing in the PICDRP limits harmed parties, regulatory authorities or law enforcement from pursuing other available remedies against the party causing harm (whether a Registry Operator, Registrar or registrant), including, for example, pursuing remedies through administrative, regulatory or judicial bodies to seek fines, damages, injunctive relief or other remedies available at law.

Section 3b, Spec 11, new gTLD Registry Agreement

Registry Operator will periodically conduct a technical analysis to assess whether domains in the TLD are being used to perpetrate security threats, such as pharming, phishing, malware, and botnets. Registry Operator will maintain statistical reports on the number of security threats identified and the actions taken as a result of the periodic security checks. Registry Operator will maintain these reports for the term of the Agreement unless a shorter period is required by law or approved by ICANN, and will provide them to ICANN upon request.

Abuse Mitigation Current Practices: ICANN

Carlos Alvarez (SSR Team)

Security, Stability and Resiliency Team

Carlos Álvarez | #ICANN57 | 4 November 2016

SSR Team, Office of the CTO

1	2	3
Capability building and Collaboration	Challenges	Aspirations

Anti-Abuse | Capability Building

- From DNS fundamentals to investigating threats to the system
  - DNSSEC trainings still ongoing
- Mostly every week throughout the year in all regions
- Recent examples:
  - US DOJ x2
  - Underground Economy
  - Austrian Cybersecurity Competency Center
  - Middle East (Doha, Dubai, Beirut x2)
  - Organization of American States
  - Organization for the Security and Cooperation in Europe
  - Latin America (Peru x2, Costa Rica, Colombia)

Anti-Abuse | Law Enforcement | Operational Security

- Reactive informal advice regarding investigations involving DNS resources
- Improve their understanding of ICANN's contractual framework related to anti-abuse provisions
- Assist in processing of Expedited Registry Security Requests
- Provide advice to staff and community, i.e. Specification 11 3(b) and registry Security Framework

Anti-Abuse | Challenges

- Registrars/registries with different systems, processes, different resource availability, different levels of expertise
- Reports of abuse not being clear, not providing enough information or being false positives – lack of standardization in abuse reporting
- Sometimes seen lack of understanding of anti-abuse provisions, both on complainants and registrars, no clear definition of what constitutes abuse

Anti-Abuse | Challenges

- No uniform ToS/AUP across registrars/registries re: anti-abuse provisions
- For anti-abuse research purposes, difficulties and repeatability in obtaining data, lack of it

Anti-Abuse - Aspirations

- A clear definition of what constitutes DNS abuse, PSWG can help (ITHI – CCTRT already include community feedback)

- Research on standardization of abuse reporting processes, aiming at making life easier for registrars and complainants

Abuse Mitigation Current Practices: gTLD Registries

Brian Cimbolic (PIR)

Statton Hammock (Rightside)

Public Interest Registry: Abuse Mitigation Measures

- Abuse mitigation begins and ends at our Anti-Abuse policy (generally Phishing, spam and malware).
- Work with our backend provider on both reactive measures and proactive measures.

Reactive Measures

- Abuse alias – Abuse@pir.org is monitored all waking hours 365 days a year. Typically respond or begin investigation within 8-12 hours at the latest.
  - If the referral occurs within our business hours, typically handled within 1-2 hours.
- Referral path – end users, LE and organizational referrers.
  - Majority of end-user referrals are not actual abuse, but people asking us to intervene with a registration for other reasons.
  - When people do refer actual abuse, it's usually spam or phishing. Occasionally we'll receive notifications from industry sources as well, particularly for malware.

Reactive - Abuse Indicated

- Refer domain and any correspondence along to registrar.
- Want to give registrar a chance to investigate, remediate, or even provide evidence to the contrary.
- When we do refer, we always tell Rr that we reserve the right to suspend if no action taken.
- If no satisfactory response received, we suspend the registration.
- Deletions have proven ineffective. There have been a few instances when we delete the registration and literally the next day the domain is re-registered and engaged in the same abusive activity.

Reactive – Law enforcement

- LEA referrals are treated with priority.
- Work with LEA to mutually refer abuse incidents and assist in providing language for court orders.

Proactive Measures

- Work closely with backend provider on proactive measures.
- Systems in place to flag unusual patterns. For instance if a registrar has huge volumes compared to its normal volume, it tells us to take a look.
- Every day get a report of previous day's registration with WHOIS information. Scan those against various black list sources.
- Once we find these, follow the same steps as reactive. We notify the registrar. Hope for registrar action but if they do not act, we do.

Abuse Mitigation Statistics

- YTD in Review nGTLDs

Anti-Abuse Efforts

Contractual Requirements

- **Rights Protection Mechanisms**
  - Sunrise Period
  - Claims Period
  - URS / UDRP
  - Sunrise Dispute Resolution Process (SDRP)

- **Public Interest Commitments – Specification 11**
  - Technical and statistical analysis of security threats
  - Regulated / Highly Regulated TLD requirements (e.g *.LAWYER*)
  - Public Interest Commitments Resolution Process (PICDRP)

Voluntary Efforts (incl. Voluntary PICS)

- **Domains Protected Mark List (DPML)**
- **Claims Plus** (extended claims period available for TMCH strings)
- **Spec 11 Security Framework**

Additional Individual Efforts

- **Trusted 3rd Parties** – IWF, NCMEC (Anti CSAM) / MPAA (copyright)
- **Healthy Domains Initiative**
- **Anti-Illegal Pharma Efforts**

Rightside®

Rightside® FACTSHEET

Number of TLDs : 40

Total Domains : 565,032*

3 **Abuse Report Sources** (Direct Reports / Domain Reputation Service Provider / IWF)

3 **Highly Regulated Top Level Domains** (.Lawyer, .Attorney, .Dentist)

0 **Public Interest Commitment Dispute Resolution Procedures**

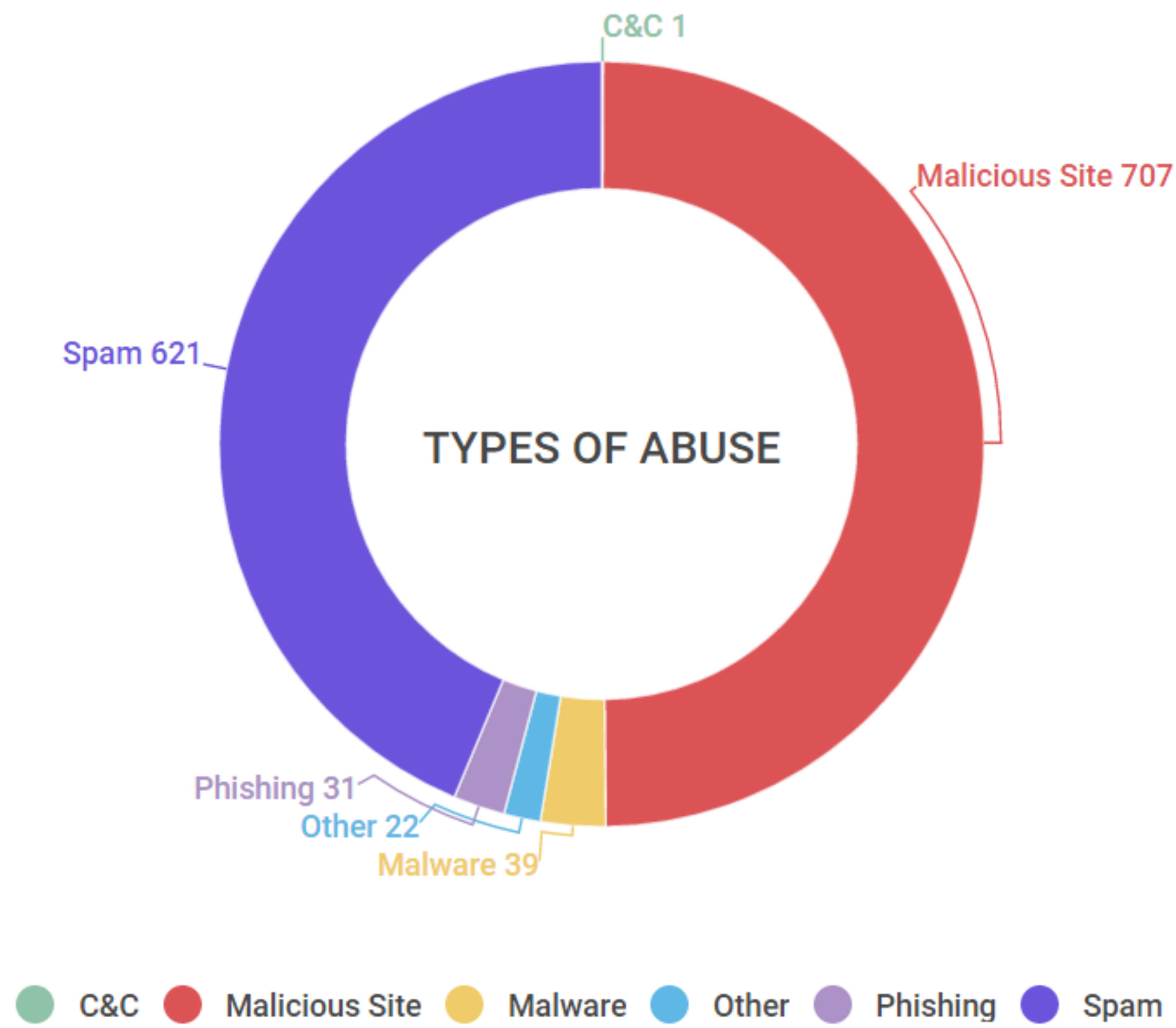
0 **Sunrise Dispute Resolution Procedures**

52 **URS proceedings initiated** (since Launch)

* Correct as of 1 November 2016

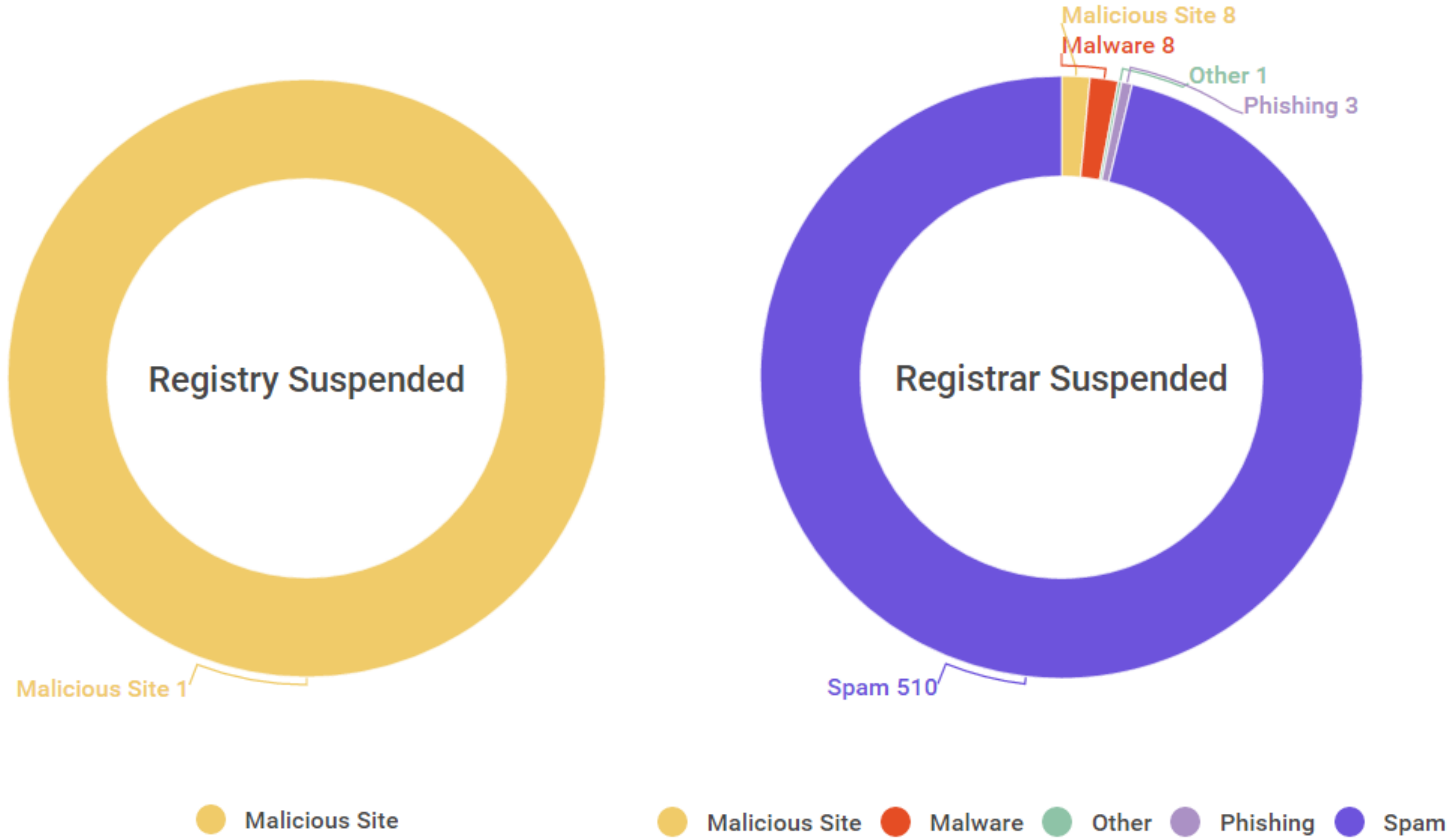
Rightside®

Abuse Types YTD 2016



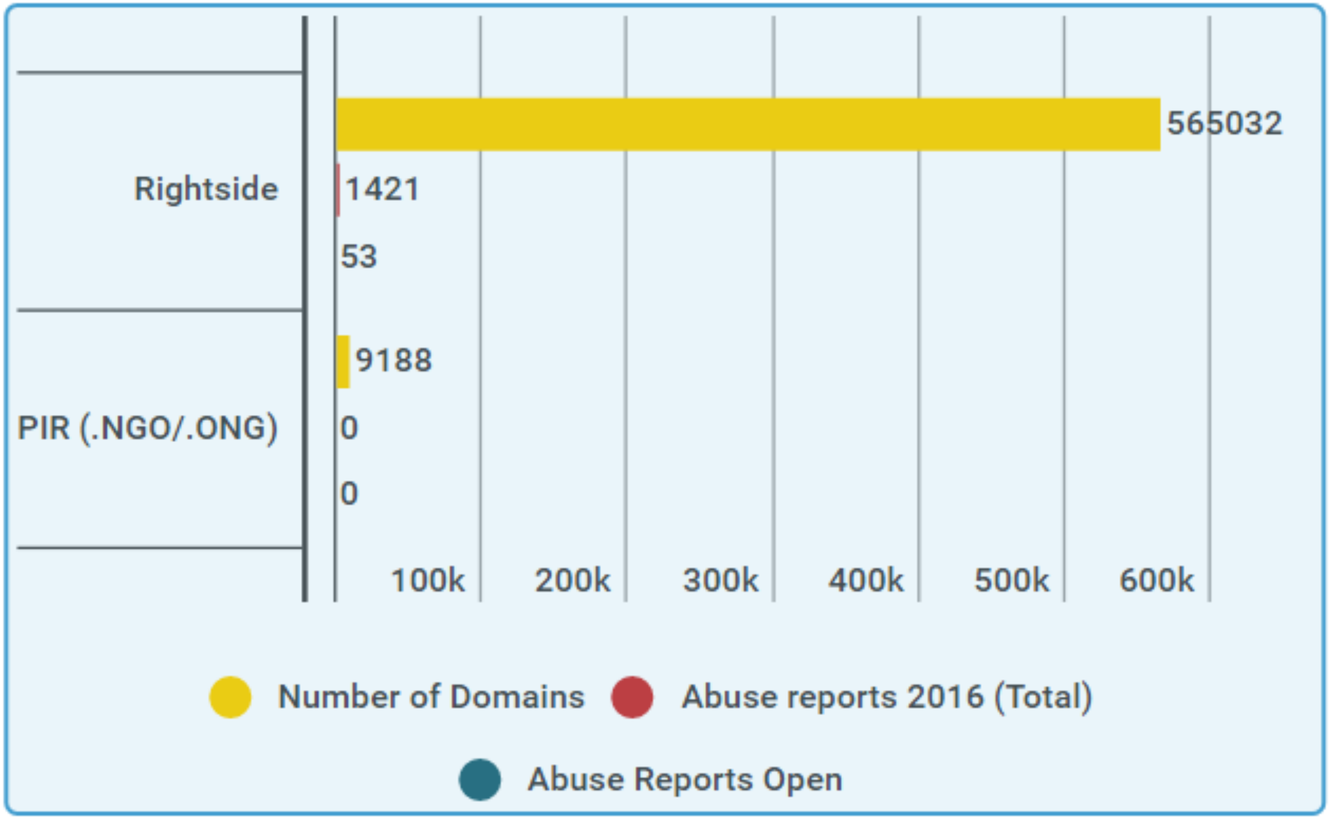
Rightside®

Domain Suspension



Rightside®

Low Levels of Reported Abuse



Abuse Mitigation
Current Practices: ccTLD Registries

Giovanni Seppia (EURid, .eu)

ICANN

EURid’ approach for abuse mitigation and prevention

ICANN57 Hyderabad

Giovanni Seppia

EURid and .eu framework

- **Initiative taken by the EC in 1999 within the *e*Europe Plan**
  Accelerating e-commerce: *«The Commission will support a .eu top level domain to encourage cross-border electronic commerce within the EU ...»*

- **EU Regulation 733/2002 created the legal framework**

- **Request for Expression of Interest in 2002**
  EURid consortium chosen in 2003

- **PPR included in the EC Regulation 874/2004**

- **EURid reappointed as the .eu registry in 2014**
  EC Implementing Decision of 11 April 2014 (2014/207/EU) on the designation of the .eu Top Level Domain Registry

.eu
Your European Identity

Procedural and technical security measures

- DNSSEC
- Registry lock
- Homoglyph bundling
- Script matching

WHOIS quality plan

- Authority of EURid is restricted to verification of registration data
- According to the EC Regulation and T&C's EURid may take action in case of abuse, but:
  - At own risk (damage claims if wrong action)
  - Assessment of "abuse": only court
- When content related, we ask registrar to take action

WHOIS quality plan

- Daily verification of registration data
  - Registry initiative:
    - Verification of legacy
    - Daily checks of new registrations
  - Third party initiative:
    - LEA (Belgian customs, Belgian Prosecutor,…)
    - Complaints
    - (automated) notifications of abuse (spam/phishing)

.eu Your European Identity

WHOIS quality plan

- Address verification:
  - Against official 3rd party database (postal addresses)
  - Against Google Maps

WHOIS quality plan

- Domain names

  - Suspended: 14 710 (holder still has the domain and it is shown in WHOIS)

  - Withdrawn: 10 128 (holder no longer has the domain but it is not shown in WHOIS)

  - Released: 6 981 (domains are available on first come first served basis)

  Total = **31 819** domain names were deleted as a result of data verification (at EURid's own initiative)

Cooperation with LEA in Belgium and registrars

- **CERT-EU (Memorandum of Understanding since three years)**
  - First hand notifications of spam/phishing/ …

- **Cybersquad (Belgian customs special cybercrime unit)**
  - Very good cooperation on counterfeit
  - In most cases, they don’t want to take down a domain, but to collect evidence of website content because they need verification of registration data and want to arrest people on the spot

- **FOD Economie (Belgian Ministry of Economic Affairs)**
  - Very good cooperation on copyright infringement (peer to peer)
  - In most cases, the need verification of registration data and want to arrest people on the spot or they request action via Public Prosecutor

- **Public Prosecutor**
  - Request for seizure of domain(s) and/or redirection to specific website or IP address (in most cases based on global cooperation with FBI / EUROPOL) (art. 39bis Criminal Code)

- **Regular cooperation with our top registrars and commitment to engage them in fighting and preventing abuses**

Research on predicting abuse

- APEWS approach
- Scope: Focused on technical abuse, more specifically C&C for botnets, spam and phishing domains, malware domains (distribution and control)
- Output of abusive prediction will be used as feed for delayed delegation

Research on predicting abuse

- 2015: project with iMinds, KU Leuven to investigate the possibility of creating a predictive model and/or method to predict abuse.

- The model is first and foremost based on the registration data and not DNS query data. Registration data is e.g.:
  - registrant data,
  - registrar “reputation”,
  - NS data,
  - #registration per registrar per registrant per unit of time
  - …

Giovanni Seppia
giovanni.seppia@eurid.eu

Abuse Mitigation Current Practices: Registrars

Michele Neylon (Blacknight)

Abuse Mitigation Current Practices: Business

Denise Michel (Facebook)

ICANN

Abuse in gTLDs

Perspectives from a Global Platform

Denise Michel
Facebook Inc.
Domain Name System (DNS)
Strategy & Management

Domain Name Volume Effect

- Few companies have the same scale and adversaries as Facebook and its family of companies.
- We do a great deal to protect our users and help secure the Internet.
- Domain names are a source of abuse AND are key to detection, deterence, and prevention on our global platforms.
- A single malicious domain name spawns numerous FQDNs* that spawn an exponential number of URLs, and our platform ends up with several orders of magnitude of "badness" or harm to users.

**fully qualified domain name: the complete domain name, includes the hostname and the domain name*).

Domain Name Abuse Challenges

Facebook constantly works to improve critical domain registration and management processes to protect our users and companies from:

- Brand Infringement
- Cybersquatting
- Phishing
- Malware
- False/Undesired Associations
- Other damaging activities

Today's Focus

Malicious or *fraudulent* domain registration and related use (e.g., domains registered in bad-faith, sometimes based on a brand name or mark, meant to confuse, deceive, or misdirect visitors -- often for phishing, spam, malware/botnet distribution and usually for profit)

Why this focus?

"… the allocation of registered names; the maintenance of and access to registration (WHOIS) information; the transfer, deletion, and reallocation of domain names …. are generally within the scope of GNSO policy-making … [and are] listed in registration agreements as being subject to Consensus Policies … " – RAPWG 2010

ICANN and the bottom up multi-stakeholder process have direct oversight and/or influence through policy-making, contracts, and related enforcement or compliance processes.

ICANN Requirement for Registrars

"Registrar will … verify … the email address of the Registered Name Holder …. by sending an email requiring an affirmative response …. or the telephone number …. by either (A) calling or sending an SMS …. providing a unique code that must be returned … or (B) calling the … telephone number and requiring the Registered Name Holder to provide a unique code …" -- *WHOIS Accuracy Program Specification*

ICANN Requirement for Registrars (cont.)

Registration agreement must include that “[a] Registered Name Holder′s willful provision of inaccurate or unreliable information ... constitute[s] a material breach of the Registered Name Holder-registrar contract and be a basis for suspension and/or cancellation of the Registered Name registration.”
– *RAA 3.7.7.2*

ICANN Requirements for Registrars (cont.)

"Registrar shall maintain an abuse contact to receive reports of abuse involving Registered Names sponsored by Registrar, including reports of Illegal Activity … [and] shall take reasonable and prompt steps to investigate and respond appropriately to any reports of abuse." – *RAA 3.18.1*

Registry Agreement

"Registry Operator will … [require] Registrars to include in their Registration Agreements a provision prohibiting Registered Name Holders from distributing malware, abusively operating botnets, phishing, piracy, trademark or copyright infringement, fraudulent or deceptive practices, counterfeiting or otherwise engaging in activity contrary to applicable law …"
-- *Specification 11 3a of the RyA*

What does this all mean?

ICANN and the bottom up multi-stakeholder process have already, through policy-making and related contracts, taken the position that abuse mitigation is required in the DNS.

Why is any of this important?

Registries and Registrars:

- Can *and* do play a gating or mitigating function in relation to DNS abuse
- Have contractual obligations to do so
- *Should* have business incentive to do so (e.g., protecting the end-user is good for protecting the DNS ecosystem and domain name registration business)

Real life example of where this plays out

- Domain names COM-VIDEO.NET and LOGIN-ACCOUNT.NET registered using Facebook's complete name and contact details
- Used for fraud attacks on Facebook network and its users:
    - Spam
    - Phishing
    - Malware
    - Targeted 30,000 Facebook users through Messenger

Facebook.com WHOIS

- Domain Name: facebook.com
- Registrant Name: Domain Administrator
- Registrant Organization: Facebook, Inc.
- Registrant Street: 1601 Willow Road,
- Registrant City: Menlo Park
- Registrant State/Province: CA
- Registrant Postal Code: 94025
- Registrant Country: US
- Registrant Phone: +1.6505434800
- Registrant Phone Ext:
- Registrant Fax: +1.6505434800
- Registrant Fax Ext:
- Registrant Email: domain@fb.com
- Registry Admin ID:
- Admin Name: Domain Administrator
- Admin Organization: Facebook, Inc.
- Admin Street: 1601 Willow Road,
- Admin City: Menlo Park
- Admin State/Province: CA
- Admin Postal Code: 94025
- Admin Country: US
- Admin Phone: +1.6505434800
- Admin Phone Ext:
- Admin Fax: +1.6505434800
- Admin Fax Ext:
- Admin Email: domain@fb.com
- Tech Name: Domain Administrator
- Tech Organization: Facebook, Inc.
- Tech Street: 1601 Willow Road,
- Tech City: Menlo Park
- Tech State/Province: CA
- Tech Postal Code: 94025
- Tech Country: US
- Tech Phone: +1.6505434800
- Tech Phone Ext:
- Tech Fax: +1.6505434800
- Tech Fax Ext:
- Tech Email: domain@fb.com
- Name Server: b.ns.facebook.com
- Name Server: a.ns.facebook.com

Login-account.net

- Registry Domain ID: 5696800_DOMAIN_COM-VRSN
- Registrar WHOIS Server: whois.onlinenic.com
- Registrar URL: http://www.onlinenic.com
- Updated Date: 2016-07-24T04:00:00Z
- Creation Date: 2016-07-24T04:00:00Z
- Registrar Registration Expiration Date: 2017-07-24T04:00:00Z
- Registrar: Onlinenic Inc
- Registrar IANA ID: 82
- Registrar Abuse Contact Email: onlinenic-enduser@onlinenic.com
- Registrar Abuse Contact Phone: +1.5107698492
- Domain Status: ok https://icann.org/epp#ok
- Registry Registrant ID:
- **Registrant Name: Domain Administrator**
- **Registrant Organization: Facebook, Inc.**
- **Registrant Street: 1601 Willow Road,**
- **Registrant City: Menlo Park**
- **Registrant State/Province: CA**
- **Registrant Postal Code: 94025**
- **Registrant Country: US**
- **Registrant Phone: +1.6505434800**
- **Registrant Phone Ext:**
- **Registrant Fax: +1.6505434800**
- **Registrant Fax Ext:**
- **Registrant Email: domain@fb.com**
- **Registry Admin ID:**
- **Name Server: ns2.dns-diy.net**
- **Admin Name: Domain Administrator**
- **Admin Organization: Facebook, Inc.**
- **Admin Street: 1601 Willow Road,**
- **Admin City: Menlo Park**
- **Admin State/Province: CA**
- **Admin Postal Code: 94025**
- **Admin Country: US**
- **Admin Phone: +1.6505434800**
- **Admin Phone Ext:**
- **Admin Fax: +1.6505434800**
- **Admin Fax Ext:**
- **Admin Email: domain@fb.com**
- **Registry Tech ID:**
- **Tech Name: Domain Administrator**
- **Tech Organization: Facebook, Inc.**
- **Tech Street: 1601 Willow Road,**
- **Tech City: Menlo Park**
- **Tech State/Province: CA**
- **Tech Postal Code: 94025**
- **Tech Country: US**
- **Tech Phone: +1.6505434800**
- **Tech Phone Ext:**
- **Tech Fax: +1.6505434800**
- **Tech Fax Ext:**
- **Tech Email: domain@fb.com**
- **Name Server: ns1.dns-diy.net**
- **Name Server: ns2.dns-diy.net**

Registrar & ICANN took 2 months …

- Scheme detected, blocked, and reported to registrar (OnlineNIC) and ICANN Compliance Team
- Took more than 2 months, dozens of communications to cancel 2 domains -- despite registrar's acknowledgement that "the current whois information of domain name does not show the correct domain owner and these domain names was used to phishing Facebook users." (*sic*) – *OnlineNIC response 8/25/16*

Lessons Learned

The system fails if:

- Registrar doesn’t do basic validation, verification at point of registration
- Registrar is inattentive to abuse reports
- Registrar is unwilling to take appropriate remedial action afforded under the RAA (in this instance, OnlinNIC insisted on obtaining the Account Holder’s approval to modify the WHOIS – the same Account Holder who perpetrated the fraudulent registrations and use of the domains in the first instance)
- ICANN Contractual Compliance closes ticket without results, and then takes “cooperative enforcement” efforts with a registrar who is non-compliant

It takes a village …

As a global platform, Facebook understands that not everything gets caught "at the gate" and abuse prevention procedures are not perfect, but our community should demand that:

- All parties employ good faith efforts to follow existing abuse prevention policies and procedures
- When procedural failures are identified, they are rectified promptly (e.g., it shouldn't take over two months to address blatant false WHOIS tied to fraudulently used domains)
- ICANN needs to address ignored or habitual system/procedural failures through appropriate contract compliance

Conclusion

We don’t have to recreate the wheel …
Abuse prevention policies and contractual obligations already exist;
implement them.

Engage with ICANN

Thank You and Questions

Reach us at:
Email: engagement@icann.org
Website: icann.org

twitter.com/icann

soundcloud.com/icann

facebook.com/icannorg

weibo.com/ICANNorg

youtube.com/user/icannnews

flickr.com/photos/icann

linkedin.com/company/icann

SlideShare
slideshare.net/icannpresentations